REPORT TO: **PENSION SUB-COMMITTEE OF THE CITY GOVERNANCE COMMITTEE & PENSION BOARD – 23 MARCH 2025**

REPORT ON: **TAYSIDE PENSION FUND INTERNAL AUDIT REPORTS – RISK MANAGEMENT FRAMEWORK REVIEW**

REPORT BY: **EXECUTIVE DIRECTOR OF CORPORATE SERVICES**

REPORT NO: **79-2026**

1 PURPOSE OF REPORT

To submit audit reports prepared by the Fund's Internal Auditor, Pricewaterhouse Coopers (PwC).

2 RECOMMENDATIONS

Members are asked to note the content of the report on the audit review undertaken, and to approve the management response.

3 FINANCIAL IMPLICATIONS

None.

4 MAIN TEXT

4.1 The report details the review undertaken that focused on Fund's Risk Management Framework for 2025/26. PwC have provided an overall rating of this area as 'Satisfactory with Exceptions' driven by four Medium-rated findings and one Low-rated finding.

PwC's review found that Tayside Pension Fund has a well-established and actively used risk management framework, with strong governance engagement, comprehensive risk registers, and regular reporting already in place. The audit confirmed that the fundamentals of risk oversight, risk articulation, and control awareness are operating effectively in practice, with clear evidence of commitment to continuous improvement.

The five findings identified relate primarily to opportunities to formalise and strengthen existing arrangements such as documenting risk ownership and escalation routes, refreshing the Risk Policy and Appetite Statement to reflect the Fund's current maturity, enhancing completeness checks and horizon scanning processes, consolidating risk reporting into a clearer single view, and developing a more structured assurance framework.

4.3 The findings and recommendations of the audit have been discussed with management and responses are contained within the report. The implementation of the agreed management actions will be monitored, with progress being reported to the Sub-Committee in due course.

5 POLICY IMPLICATIONS

This report has been subject to the Pre-IIA Screening Tool and does not make any recommendations for change to strategy, policy, procedures, services or funding and so has not been subject to an Integrated Impact Assessment. An appropriate senior manager has reviewed and agreed with this assessment.

6 CONSULTATIONS

The Chief Executive and Head of Democratic and Legal Services has been consulted on the content of this report and agree with the contents.

7 BACKGROUND PAPERS

None

PAUL THOMSON
EXECUTIVE DIRECTOR OF CORPORATE SERVICES **27 MARCH 2026**

Internal audit report 2025/26

Risk Management Framework Review

Tayside Pension Fund (TPF)

Final Report

PwC

March 2026

Contents

Distribution list

For action:
Stuart Norrie (Senior Banking & Investment Officer)
Pradipta Mohanty (Service Manager - Financial Services)

Executive summary

Report classification

Satisfactory with Exceptions

Refer to Appendix A for the basis of classification

Total number of findings	Critical	High	Medium	Low	Advisory
5	0	0	4	1	0

Background and Scope

An effective risk management framework is fundamental to ensuring that the Fund meets its long-term objectives — namely safeguarding members' benefits, maintaining employer contribution stability, and supporting sound decision-making. As TPF operates within the Local Government Pension Scheme (LGPS) framework, it is required to identify, assess, manage and monitor risks in a prudent, transparent, and proportionate manner.

While TPF has established governance arrangements and documented elements of its risk framework, effective risk management requires the Fund to retain clear ownership and oversight of risk management activities. This includes:

- Clearly articulating the Fund's risk strategy, risk appetite, and governance framework.
- Defining roles, responsibilities, and escalation routes across officers, committees, and the Pension Board.
- Ensuring risks are consistently identified, assessed, monitored and reported, with appropriate assurance over key controls and third-party arrangements.

In an increasingly complex regulatory and operating environment, strong risk governance is critical. In line with the Pensions Regulator's General Code, effective risk management supports:

- Clear accountability and delegation for risk management and oversight.
- Robust challenge and scrutiny of key risks to ensure alignment with the Fund's objectives and risk appetite.
- Transparent and defensible risk-based decisions, providing assurance to employers, members, auditors and regulators.
- Ongoing review and adaptation of the risk framework to reflect changes in the Fund's activities and external environment.

Summary

The overall rating of this report is Satisfactory with exceptions, driven by four 'medium' rated findings and one 'low' rated finding. The scope of this review and our findings are summarised in the table below. Full details, alongside agreed actions from management are within the body of the report.

Executive summary

Summary of findings

Scope		Summary of findings
Governance and Oversight	• There are clear, single points of accountability for each key risk, with defined responsibilities and escalation paths. • Committees responsible for risk oversight are appropriately governed, with Terms of Reference, defined membership, and evidence of effective functioning (e.g., minutes, actions). • Governance and escalation routes to the Risk Committee (or Board) are documented and used, with actions clearly tracked through to resolution.	**Finding 1: Enhancing risk governance oversight (Medium)-** The Fund's risk governance arrangements operate in practice but would benefit from greater formalisation to support clearer accountability, escalation, and follow-up of risk matters. Current arrangements rely on established reporting routines rather than a clearly documented governance framework. **Key aspects where governance discipline could be strengthened include:** • Explicit assignment of ownership for key risks. • Clearly documented escalation routes and thresholds. • Formal tracking of actions arising from risk discussions. Enhancing governance structure in these areas would support more consistent oversight and timely resolution of risk issues.
Risk Policy & Appetite	• A formally approved and periodically reviewed risk management policy exists and is aligned with the TPF's objectives and regulatory expectations. • TPF's risk appetite and tolerances are clearly defined, documented, and communicated to relevant stakeholders. • Risk appetite is linked to key decision areas such as investment, funding, operations, and covenant strength, and reviewed at least annually.	**Finding 2: Inconsistent articulation of risk policy and appetite (Medium)-** Fund has an established Risk Management Policy and documented risk appetite; however, the framework has not been updated to clearly explain how appetite should be interpreted, governed, and applied as risk practices have evolved. **Key areas requiring clearer articulation include:** • How risk appetite informs governance oversight and escalation. • The relationship between documented appetite and decision-making. • Formal confirmation and validation of appetite over time. Clarifying these aspects would improve consistency and transparency in the application of risk appetite.
Risk Identification & Assessment	• The risk register includes all relevant risks (strategic, operational, financial, regulatory, ESG) and is regularly updated. • Risk descriptions, causes, impacts, and controls are clearly articulated and consistently captured. • There is a structured process for identifying emerging risks (e.g., horizon scanning, workshops), and these are reviewed by relevant committees.	**Finding 3: Limited maturity in the risk identification and assessment framework (Medium)**- The Fund maintains a comprehensive Risk Register with a consistent structure; however, risk identification and assessment rely largely on periodic review rather than a clearly defined, forward-looking framework. **Key limitations in the current approach include:** • Absence of explicit confirmation that all relevant risk categories are captured. • Informal identification of emerging risks without structured horizon scanning. • Variable depth and clarity in risk control descriptions. Introducing greater structure would support a more robust and future-focused assessment of risk

Executive summary

Summary of findings

Scope		Summary of findings
Risk Monitoring & Reporting	• Risk reports are produced regularly, include forward-looking insights, and cover key risk metrics (KRIs), risk ratings, and trends. • Action plans from prior risk assessments are clearly tracked, with assigned owners and due dates. • Risk dashboards and reporting are integrated with other performance and compliance reports where appropriate.	**Finding 4: Limited integration and visibility across risk reporting (Medium)-** Risk information is routinely reported to governance bodies but is presented across multiple reports without a consolidated or forward-looking risk view. This reduces visibility of the Fund's overall risk profile. **Key weaknesses in the current reporting approach include:** • Lack of a single risk dashboard or consolidated risk report. • Absence of defined Key Risk Indicators and trend analysis. • Limited linkage between risk reporting, performance reporting and incident management. A more integrated reporting approach would enhance transparency and support more effective oversight.
Risk Mitigation & Controls	• Key controls are documented for each significant risk and reviewed periodically for design and operating effectiveness. • There is a formal process to assess the effectiveness of controls (e.g. self-assessment, internal assurance, third-party review). • The scheme has visibility of and assurance over third-party or outsourced controls (e.g. administrators, investment managers).	**Finding 5: Inconsistency in Control Assurance arrangements (Low)**- Controls are documented and assurance is obtained from multiple sources; however, there is no unified framework to consistently assess, evidence, and track control effectiveness across the Fund and its outsourced arrangements. **Key gaps in the assurance approach include:** • No formal assessment of control design or operating effectiveness. • Inconsistent ownership and accountability for controls. • Lack of a scheme-owned approach to third-party assurance and follow-up. A more structured assurance framework would improve confidence in the effectiveness of the control environment.

Current year findings

1 Enhancing risk governance oversight

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Finding and root cause

TPF has established governance bodies and regular reporting arrangements to support risk oversight; however, the design of governance and oversight arrangements does not clearly define accountability, escalation, and follow-up mechanisms for risk management. Specifically:

- Individual risk ownership is not explicitly documented, resulting in unclear roles and responsibilities for managing and escalating risks.
- Escalation thresholds, routes, and follow-up arrangements are not formally defined within a consolidated governance framework, with escalation relying primarily on routine reporting cycles.
- Actions arising from risk governance forums are not centrally tracked, with follow-up relying on subsequent agenda items rather than a formal action log.
- Lack of formally approved Pension Sub Committee Terms of Reference to articulate risk-specific responsibilities including key elements like Purpose and Objective, Membership details, Voting rights for decision making, Delegation details if any, Regular MI expectations and other Ad-Hoc reporting.

Potential implications

In the absence of clearly defined risk ownership, escalation criteria, and formal action-tracking arrangements, there is a risk that key risks are not escalated, challenged, or mitigated in a timely and consistent manner. This may lead to unclear accountability, reliance on informal practices, and reduced assurance that governance and oversight arrangements operate effectively and consistently.

Recommendations

1. Define and document clear ownership for key risks, including roles and responsibilities for managing and escalating risks.
2. Develop and formalise a consolidated risk governance framework, setting out escalation thresholds, routes, and oversight responsibilities to support consistent and timely escalation to the Pension Sub-Committee and Board.
3. Introduce a centralised action-tracking mechanism to record risk-related actions, ownership, due dates, and closure.
4. Formally approve and update the Pension Sub-Committee Terms of Reference to clearly define its risk oversight responsibilities, governance arrangements, and reporting expectations

Current year findings

1 Enhancing risk governance oversight

Control Design

Management action plan

All the above recommendations will be implemented on or before the target date.

Responsible person/title:

Pradipta Mohanty
Service Manager- Financial Services

Target date:

31st December 2026

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Current year findings

2 Inconsistent articulation of risk policy and appetite

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Finding and root cause

TPF has an approved Risk Management Policy & Strategy and a documented Risk Appetite Statement, and risk appetite is applied within the Risk Register. However, as the Fund's risk management practices have evolved over time, the Risk Policy and Appetite framework has not been refreshed to clearly articulate how risk appetite should be interpreted, governed, and embedded across decision-making and oversight, resulting in gaps in clarity and consistency. Specifically:

- The Risk Management Policy has not been substantively refreshed to reflect the enhanced maturity now evident in practice, including the use of explicit appetite markers and inherent and residual risk scoring.
- The Policy does not explicitly reference alignment to the TPR General Code (ESOG), relying instead on implicit compliance through governance practices.
- Risk appetite is defined qualitatively, with no quantified tolerances or thresholds for key risk areas.
- While risk appetite is recorded in the Risk Register, the Policy does not clearly articulate how appetite should be interpreted, applied in governance processes, or explicitly linked to strategic decision-making and escalation.
- There is no explicit requirement for standalone annual confirmation or validation of risk appetite, nor for periodic validation that the Risk Register remains aligned with the approved Risk Policy and Appetite Statement.

Potential implications

In the absence of a clearly articulated and up-to-date Risk Policy and Appetite framework, there is a risk that risk appetite is not interpreted or applied consistently across governance and decision-making activities. Reliance on qualitative definitions and implicit practices may reduce transparency over how risk appetite is intended to inform escalation, challenge, and oversight, and may limit the Fund's ability to clearly demonstrate alignment between its documented policy, evolving risk practices, and regulatory good-practice expectations.

Current year findings

2 Inconsistent articulation of risk policy and appetite

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Recommendations

1. Refresh and formally approve the Risk Management Policy & Risk Appetite Statement to reflect current risk management practices (including appetite markers and inherent/residual scoring) and to clearly articulate governance expectations.
2. Explicitly reference alignment to relevant regulatory good practice (including the TPR General Code) within the Risk Policy to enhance transparency and defensibility.
3. Clearly define how risk appetite should be interpreted, applied, and linked to governance decision-making and escalation, including consideration of whether defined tolerances are appropriate for key risk areas.
4. Introduce a structured validation process to periodically confirm alignment between the Risk Policy, Risk Appetite Statement, and the Risk Register.
5. Establish formal annual confirmation of risk appetite through the governance cycle to ensure it remains appropriate as conditions evolve.

Management action plan

All the above recommendations will be implemented on or before the target date.

Responsible person/title:

Pradipta Mohanty
Service Manager- Financial Services

Target date:

31st December 2026

Current year findings

3 Limited maturity in the risk identification and assessment framework

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Finding and root cause

TPF maintains a comprehensive Risk Register and applies a broadly consistent structure to risk documentation; however, the design of the risk identification and assessment framework does not fully demonstrate completeness, consistency, or a clearly defined, forward-looking approach to identifying and assessing risks as the Fund's activities evolve. Specifically:

- There is no explicit confirmation of completeness of the Risk Register against a defined risk taxonomy.
- Identification of emerging risks is informal and source-driven, with no documented horizon-scanning framework, structured methodology, or clear distinction between emerging and established risks.
- While risks follow a common structure, the depth and clarity of control descriptions varies, and linkage between controls and risk mitigation is not always explicit.
- There is no documented quality assurance or validation process to periodically assess the consistency, clarity, or completeness of risk descriptions, causes, impacts, and controls.
- The Risk Management Policy does not clearly set minimum documentation standards or require periodic validation that the Risk Register remains aligned to the Fund's evolving risk profile.
- Risk reviews and updates are primarily time-based (quarterly), with no defined triggers linked to material events or changes in the operating environment.

Potential implications

In the absence of a clearly defined and forward-looking risk identification and assessment framework, there is a risk that emerging or evolving risks are not identified, assessed, or escalated in a timely and consistent manner. Reliance on time-based reviews and informal inputs may reduce assurance that the Risk Register remains complete and current as the Fund's activities and external environment change, potentially limiting the effectiveness of risk oversight and decision-making.

Current year findings

3 Limited maturity in the risk identification and assessment framework

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Recommendations

1. Define and document a clear risk taxonomy to support periodic validation that the Risk Register remains complete and aligned to the Fund's risk universe.
2. Formalise an emerging-risk identification process, including horizon scanning and structured consideration of internal and external inputs.
3. Establish minimum documentation standards for risk descriptions, causes, impacts, and controls to improve consistency and transparency including clearer linkage between controls and risk mitigation.
4. Implement a light-touch quality assurance process to periodically review the completeness and consistency of risk documentation across the Risk Register
5. Update the Risk Management Policy to define minimum documentation expectations and require periodic validation that the Risk Register reflects the Fund's evolving activities and risk profile.
6. Define event-driven review triggers to supplement quarterly reviews and ensure risks are reassessed following material changes in the operating or regulatory environment.

Management action plan

All the above recommendations will be implemented on or before the target date.

Responsible person/title:

Pradipta Mohanty
Service Manager- Financial Services

Target date:

31st December 2026

Current year findings

4 Limited integration and visibility across risk reporting

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Finding and root cause

TPF produces regular governance reporting and risk-related information across multiple reports; however, the design of the risk monitoring and reporting framework does not provide a consolidated, structured, or forward-looking view of risk across the Fund, nor clearly support accountability and follow-up of risk responses. Specifically:

- There is no standalone or consolidated risk report or dashboard providing a single, coherent view of the Fund's overall risk profile and related risk metrics.
- Key Risk Indicators (KRIs) are not explicitly defined, documented, or reported, and trends in risk exposure are not formally analysed or presented.
- Risk reporting is distributed across multiple reports, with integration with performance and compliance information occurring through co-presentation rather than structured linkage.
- Risk mitigation actions arising from risk monitoring are not formally tracked through a structured action log with clearly defined ownership, due dates, and follow-up, resulting in implicit accountability and limited visibility over completion status.
- There is no formal incident management process, nor a defined mechanism to assess and reflect the impact of incidents or breaches on the Fund's risk profile or risk appetite.

Potential implications

In the absence of a consolidated and forward-looking risk reporting framework, there is a risk that senior decision-makers do not have a clear, timely, and complete view of the Fund's overall risk profile. Fragmented reporting, lack of defined risk metrics, and limited action tracking may reduce transparency over emerging risks, weaken accountability for mitigation actions, and limit assurance that risks are being effectively monitored and managed in line with the Fund's risk appetite.

Current year findings

4 Limited integration and visibility across risk reporting

Control Design

Finding rating

Impact	4
Likelihood	iv
Rating	Medium

Recommendations

1. Develop a consolidated risk reporting framework, including a single risk report or dashboard to provide a coherent view of the Fund's overall risk profile and key metrics
2. Define and implement a set of Key Risk Indicators (KRIs), supported by structured trend analysis, to enable more forward-looking monitoring of risk exposure.
3. Enhance integration between risk, performance, and compliance reporting, through clearer linkage or structured cross-referencing within governance reports.
4. Introduce a centralised action-tracking mechanism to record mitigation actions, ownership, due dates, and closure status to strengthen accountability and oversight.
5. Establish a proportionate incident management process, including a defined approach to assessing and recording the impact of incidents or breaches on the Fund's risk profile and risk appetite.

Management action plan

All the above recommendations will be implemented on or before the target date.

Responsible person/title:

Pradipta Mohanty
Service Manager- Financial Services

Target date:

31st December 2026

Current year findings

5 Inconsistency in Control Assurance arrangements

Control Design

Finding rating

Impact	3
Likelihood	iii
Rating	Low

Finding and root cause

TPF documents controls against key risks and obtains assurance through internal audit, external audit, and third-party reviews. However, the control effectiveness and assurance framework is not clearly defined or applied in a consistent and manner, limiting the Fund's ability to demonstrate how control design and operating effectiveness are assessed and monitored across the organisation. Specifically:

- While controls are documented, there is no formal process to assess or record control design effectiveness, with reliance placed on implicit review through risk discussions.
- Operating effectiveness of controls is not formally tested or documented, with no evidenced RCSA, control framework, or structured control testing programme.
- Ownership and accountability for individual controls are not consistently defined, reducing clarity over responsibility for control performance.
- Assurance activities (internal audit, external audit, and third-party reviews) provide periodic and selective coverage, rather than a routine, scheme-wide view of control effectiveness.
- There is no documented, scheme-owned framework for third-party assurance, including clear minimum expectations and follow-up arrangements for key outsourced service providers such as investment managers, the global custodian, and pensions administration systems.
- Issues identified through audit or third-party assurance are not systematically tracked, with no consistent process to record actions, ownership, and closure.

Potential implications

In the absence of a clearly defined and consistent control effectiveness and assurance framework, there is a risk that management and governance bodies lack sufficient transparency and assurance over whether key controls—particularly those operated internally and by third parties—are designed and operating effectively. This may reduce confidence in the Fund's ability to identify control weaknesses promptly, address assurance issues consistently, and demonstrate robust oversight across its control environment.

Current year findings

5 Inconsistency in Control Assurance arrangements

Control Design

Finding rating

Impact	3
Likelihood	iii
Rating	Low

Recommendations

1. Establish a defined control assurance framework that sets out how control design and operating effectiveness are to be assessed and evidenced across key risks.
2. Introduce a proportionate approach to control testing (e.g. RCSA or targeted control reviews) to support periodic assessment of control effectiveness.
3. Clarify ownership and accountability for key controls, including responsibility for monitoring and remediation.
4. Develop a structured assurance plan or framework to improve visibility over coverage and gaps across key controls.
5. Define minimum assurance expectations for key outsourced service providers, including investment managers, the global custodian and pensions administration systems.
6. Implement a structured process to track assurance findings and follow-up actions through to resolution.

Management action plan

All the above recommendations will be implemented on or before the target date.

Responsible person/title:

Pradipta Mohanty
Service Manager- Financial Services

Target date:

31st December 2026

Appendices

Appendix A: Basis of our classifications
Appendix B: Terms of reference
Appendix C: Limitations and responsibilities

Appendix A: Basis of our classifications

Individual finding ratings

Findings are assessed on their impact and likelihood based on the assessment rationale in the tables below.

Impact rating	Assessment rationale
6	A finding that could have a: • Critical impact on operational performance; or • Critical monetary or financial statement impact; or • Critical breach in laws and regulations that could result in material fines or consequences; or • Critical impact on the reputation or brand of the organisation which could threaten its future viability.
5	A finding that could have a: • Significant impact on operational performance; or • Significant monetary or financial statement impact; or • Significant breach in laws and regulations resulting in large fines and consequences; or • Significant impact on the reputation or brand of the organisation.
4	A finding that could have a: • Major impact on operational performance; or • Major monetary or financial statement impact; or • Major breach in laws and regulations resulting in significant fines and consequences; or • Major impact on the reputation or brand of the organisation.
3	A finding that could have a: • Moderate impact on the organisation's operational performance; or • Moderate monetary or financial statement impact; or • Moderate breach in laws and regulations with moderate consequences; or • Moderate impact on the reputation of the organisation.

Appendix A: Basis of our classifications

Individual finding ratings

Impact rating	Assessment rationale
2	A finding that could have a: • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organisation.
1	A finding that could have a: • Insignificant impact on the organisation's operational performance; or • Insignificant monetary or financial statement impact; or • Insignificant breach in laws and regulations with little consequence; or • Insignificant impact on the reputation of the organisation.
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.

Likelihood

Likelihood rating	Assessment rationale
vi	Has occurred or probable in the near future
v	Possible in the next 12 months
iv	Possible in the next 1-2 years
iii	Possible in the medium term (2-5 years)
ii	Possible in the long term (5-10 years)
i	Unlikely in the foreseeable future

Appendix A: Basis of our classifications

Finding rating

This grid is used to determine the overall finding rating. Issues with a low impact and likelihood rating will not be reported.

	Impact rating					
Likelihood rating	**6**	**5**	**4**	**3**	**2**	**1**
vi	Critical	Critical	High	High	Medium	Medium
v	Critical	High	High	Medium	Medium	Low
iv	High	High	Medium	Medium	Low	Low
iii	High	Medium	Medium	Low	Low	Low
ii	Medium	Medium	Low	Low	Low	Not reportable
i	Medium	Low	Low	Low	Not reportable	Not reportable

Report classifications

The report classification is determined by allocating points to each of the findings included in the report.

Findings rating	Points
Critical	40 points per finding
High	10 points per finding
Medium	3 points per finding
Low	1 point per finding

Report classification		Points
Satisfactory		6 points or less
Satisfactory with exceptions		7 – 15 points
Needs improvement		16 – 39 points
Unsatisfactory		40 points and over

Appendix B: Audit scope and approach

Scope

Our scope will consist of the following:

Sub-process	Objectives and areas of review	Risks
Governance & Oversight	• There are clear, single points of accountability for each key risk, with defined responsibilities and escalation paths. • Committees responsible for risk oversight are appropriately governed, with Terms of Reference, defined membership, and evidence of effective functioning (e.g., minutes, actions). • Governance and escalation routes to the Risk Committee (or Board) are documented and used, with actions clearly tracked through to resolution.	• Lack of accountability or ownership of risk management may lead to unmanaged risks or delays in response. • Ineffective or duplicated committee structures could lead to poor oversight and delayed decisions. • Poor escalation or follow-up of risks may result in unresolved issues or missed opportunities for mitigation.
Risk Strategy	• A formal risk strategy is in place that aligns with the TPF's long-term objectives, including funding, investment, and covenant strength. • The risk strategy is informed by scenario analysis, stress testing, and external environment scanning (e.g. market, regulatory, economic changes). • There is evidence that the risk strategy informs and guides key business decisions, including investment strategy, liability management, and journey planning. • The strategy is reviewed at least annually or in response to material events, and changes are approved by the Board or delegated committee.	• Absence of a defined risk strategy may result in misalignment between risk-taking and strategic goals. • Risk strategy does not reflect current or potential future risks (e.g. inflation, interest rate volatility, climate risks). • Key decisions are made in isolation without reference to agreed risk tolerances or long-term targets. • Risk strategy becomes outdated or irrelevant, leading to unmanaged or excessive risk exposures.
Risk Policy & Appetite	• A formally approved and periodically reviewed risk management policy exists and is aligned with the TPF's objectives and regulatory expectations. • TPF's risk appetite and tolerances are clearly defined, documented, and communicated to relevant stakeholders. • Risk appetite is linked to key decision areas such as investment, funding, operations, and covenant strength, and reviewed at least annually.	• The policy is outdated or not aligned with current practices, leading to inconsistencies in risk handling. • Risk appetite is either too vague or not known by decision-makers, leading to either over-cautious or excessive risk. • Disconnected risk appetite and strategic decisions may result in breaches or missed targets.

Appendix B: Audit scope and approach

Scope

Our scope will consist of the following:

Sub-process	Objectives and areas of review	Risks
Risk Identification & Assessment	• The risk register includes all relevant risks (strategic, operational, financial, regulatory, ESG) and is regularly updated. • Risk descriptions, causes, impacts, and controls are clearly articulated and consistently captured. • There is a structured process for identifying emerging risks (e.g., horizon scanning, workshops), and these are reviewed by relevant committees.	• Key risks are omitted or poorly documented, exposing the scheme to unexpected or unmanaged events. • Incomplete or inconsistent entries in the register lead to ineffective mitigation planning. • Failure to identify emerging risks (e.g. cyber, climate, geopolitical) could leave the scheme vulnerable to new threats.
Risk Monitoring & Reporting	• Risk reports are produced regularly, include forward-looking insights, and cover key risk metrics (KRIs), risk ratings, and trends. • Action plans from prior risk assessments are clearly tracked, with assigned owners and due dates. • Risk dashboards and reporting are integrated with other performance and compliance reports where appropriate.	• Reports are backward-looking, overly technical, or fail to provide actionable insights. • Actions are not followed through or responsibility is unclear, leading to repeated or unaddressed risks. • Siloed reporting leads to missed interdependencies or opportunities to address risks holistically.
Risk Mitigation & Controls	• Key controls are documented for each significant risk and reviewed periodically for design and operating effectiveness. • There is a formal process to assess the effectiveness of controls (e.g. self-assessment, internal assurance, third-party review). • The scheme has visibility of and assurance over third-party or outsourced controls (e.g. administrators, investment managers).	• Controls may exist but are either ineffective or not tested, exposing the scheme to unmanaged risk. • Over Reliance on undocumented or assumed controls may result in false assurance. • Inadequate oversight of third parties could lead to operational failures or regulatory breaches.

Appendix B: Audit scope and approach

Limitations of scope

As part of our review, we will not cover the following:

- Independent re-assessment or re-scoring of risks in the risk register
- Challenge or assessment of the appropriateness of your risk appetite thresholds or risk related metrics
- Detailed assessment of the management of each relevant risk types at a granular level, for instance in cybersecurity, data protection, third party, operational, climate, ESG and regulatory risks
- Accuracy and completeness of the underlying MI data
- External benchmarking or peer comparison of risk management frameworks

Our assessment will include those matters that we consider relevant based on our understanding of the key risks to the organisation. Our review will be restricted to evaluating the design effectiveness of processes and controls in place in respect to risk management.

Any observations we may report are limited to those identified through the course of our work and are not intended to represent an exhaustive list of all potential issues or considerations. Our work is not designed to ensure compliance with all laws and regulations. Fraud, error, or non compliance with laws and regulations may occur and not be detected. Furthermore, the scope of our work does not constitute assurance over compliance with any laws and regulations.

Audit approach

Our audit approach is as follows:

1. We will evaluate the processes in place to address the key risks identified on page 4 and 5 through walkthroughs with key personnel and review of documentation. This will be through discussions with key personnel, a desktop review of documentation and our knowledge of best practice.
2. Identify the key risks relating to the risk management framework, objectives and governance framework.
3. Evaluate the design of the controls in place to address the key risks.

Appendix C: Limitations and responsibilities

Limitations inherent to the internal auditor's work

We have undertaken this review subject to the limitations outlined below:

Internal control

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls, and the occurrence of unforeseeable circumstances.

Future periods

Our assessment of controls is at January 2026 only. Historic evaluation of effectiveness is not relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in operating environment, law, regulation, or other changes; or
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of management and internal auditors

It is management's responsibility to develop and maintain sound systems of risk management, internal control, and governance, and for the prevention and detection of irregularities and fraud. Internal audit work should not be seen as a substitute for management's responsibilities for the design and operation of these systems.

We endeavor to plan our work so that we had a reasonable expectation of detecting significant control weaknesses and, if detected, we carried out additional work directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected.

Accordingly, our examinations as internal auditors should not be relied upon solely to disclose fraud, defalcations, or other irregularities which may exist.

Thank you

pwc.com